CLAIMS

What is claimed is:

1. A method of securely processing a digital signal comprising:
   a) generating a public encryption key for use with a first logical circuit and a second logical circuit separate from said first logical circuit;
   b) accessing an encrypted signal at said first logical circuit;
   c) determining a first decryption key for said encrypted signal at said second logical circuit;
   d) encrypting said first decryption key at said second logical circuit by use of said public encryption key;
   e) transferring said encrypted first decryption key from said second logical circuit to said first logical circuit over a communication link;
   f) at said first logical circuit, decrypting said encrypted first decryption key by use of a secret key to determine said first decryption key; and
   g) at said first logical circuit, decrypting said encrypted signal using said first decryption key.

2. The method of Claim 1 wherein a) comprises generating said public encryption key using the technique of Diffie-Hellman Key Exchange.

3. The method of Claim 1 wherein d) comprises:

   d1) accessing said public encryption key from a first portion of local memory at said second logical circuit;

d2) accessing a computer control program from a second portion of local memory at said second logical circuit; and

d3) executing said computer control program at said second logical circuit to encrypt said first decryption key using said public encryption key.

4. The method of Claim 1 wherein d) comprises:

d1) accessing said public encryption key from a first portion of local memory at said second logical circuit;

d2) replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program;

d3) accessing said new computer control program from said second portion of local memory; and

d4) executing said new computer control program at said second logical circuit to encrypt said first decryption key using said public encryption key.

5. The method of Claim 1 wherein f) comprises:

f1) accessing a second decryption key from a first portion of local memory at said first logical circuit;

f2) accessing a computer control program from a second portion of local memory at said first logical circuit; and

f3) executing said computer control program to decrypt said first decryption key using said second decryption key.

6. The method of Claim 1 wherein f) comprises:

f1) accessing a second decryption key from a first portion of local memory at said first logical circuit;

f2) replacing a computer control program stored in a second portion of local memory at said first logical circuit with a new computer control program;

f3) accessing said new computer control program from said second portion of local memory; and

f4) executing said new computer control program at said second logical circuit to decrypt said first decryption key using said second decryption key.

7. The method of Claim 1 wherein said digital signal is substantially compliant with the Motion Pictures Experts Group (MPEG) format.

8. A method of securely processing a digital signal comprising:

a) generating a first public encryption key for use with a first logical circuit and a second logical circuit, and generating a second public encryption key for use with said first logical circuit and a third logical circuit;

b) generating a local encryption key and a local decryption key at said first logical circuit;

c) at said first logical circuit, encrypting said local encryption key by use of said first public encryption key and encrypting said local decryption key by use of said second public encryption key;

d) transferring said encrypted local encryption key to said second logical circuit and transferring said encrypted local decryption key to said third logical circuit across a communication link;

e) decrypting said encrypted local encryption key at said second logical circuit and decrypting said encrypted local decryption key at said third logical circuit; and

f) transferring said digital signal in encrypted form from said second logical circuit to said third logical circuit across a second communication link.

9. The method of Claim 8 wherein f) comprises:

f1) encrypting said digital signal at said second logical circuit using said local encryption key;

f2) transferring said digital signal in encrypted form across said second communication link between said second logical circuit and said third logical circuit; and

f3) decrypting said encrypted form of said digital signal at said third logical circuit using said local decryption key.

10. The method of Claim 8 wherein e) comprises:

e1) decrypting said encrypted local encryption key at said second logical circuit using said first public encryption key; and

e2) decrypting said encrypted local decryption key at said third logical circuit using said second public encryption key.

11. The method of Claim 8 wherein c) comprises:

c1) accessing said first public encryption key from a first portion of local memory of said first logical circuit; and

c2) accessing a computer control program from a second portion of local memory of said first logical circuit; and

c3) executing said computer control program on said first logical circuit to encrypt said first local encryption key.

12. The method of Claim 8 wherein c) comprises:

c1) accessing said first public encryption key from a first portion of local memory of said first logical circuit;

c2) replacing a computer control program stored in a second portion of local memory at said first logical circuit with a new computer control program;

c3) accessing said new computer control program from said second portion of local memory; and

c4) executing said new computer control program on said first logical circuit to encrypt said first local encryption key.

13. The method of Claim 8 wherein a) comprises generating said first public encryption key and said second public encryption key using the technique of Diffie-Hellman Key Exchange.

14. The method of Claim 8 wherein e) comprises:

e1) accessing a decryption key from a first portion of local memory of said second logical circuit;

e2) accessing a computer control program from a second portion of local memory of said second logical circuit; and

e3) executing said computer control program on said second logical circuit to decrypt said local encryption key.

15. The method of Claim 8 wherein e) comprises:

e1) accessing a decryption key from a first portion of local memory of said second logical circuit;

e2) replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program;

e3) accessing said new computer control program from said second portion of local memory; and

e4) executing said new computer control program on said second logical circuit to decrypt said local encryption key.

16. The method of Claim 8 wherein the encryption of said digital signal at said second logical circuit and the decryption of said encrypted digital signal at said third logical circuit are conducted in accordance with the procedures of the Data Encryption Standard.

17. A system for processing a secure digital signal, comprising:

a first logical circuit for decrypting a local encryption key, said first logical circuit comprising a local processor and local memory; and

a second logical circuit for encrypting said digital signal using said local encryption key accessed from said first logical circuit.

18. The system of Claim 17, further comprising a computer control program contained within said first logical circuit, said computer control program for controlling said local processor and for receiving said encryption key in an encrypted form and for decrypting said encryption key prior to providing said encryption key to said second logical circuit.

19. The system of Claim 17, further comprising a modifiable local memory contained within said first logical circuit, said modifiable local memory enabling the modification of a computer control program stored within said local memory.

20. The system of Claim 17, further configured such that the contents of said local memory cannot be observed from outside of said first logical circuit.

21. A method of securely processing a digital signal comprising:

a) monitoring said digital signal for a message to modify an encryption technique used in managing encryption keys used in processing said digital signal;

b) accessing said message;

c) interpreting said message; and

d) modifying said encryption technique in accordance with said message, wherein said encryption technique is used to manage encryption keys used in processing said digital signal.

22. The method of Claim 21 wherein d) comprises modifying the parameters for generating a public key.

23. The method of Claim 21 wherein d) comprises modifying a computer control program for generating a public key.

24. The method of Claim 21 wherein d) comprises modifying a computer control program to encrypt keys.

25. The method of Claim 21 wherein b) comprises accessing said message from a digital video cable signal provided by a Multiple Service Operator.